CLAIMS

What is Claimed is:

1. A conditional access module, comprising:

a microprocessor;

a non-volatile reprogrammable memory communicatively coupled to the microprocessor via a first communication path, the non-volatile memory for storing microprocessor program instructions; and

a logical module, communicatively coupled to the non-volatile memory via a second communication path independent from the first communication path, the logical module for verifying the data stored in the non-volatile reprogrammable memory by comparison of the contents of the non-volatile reprogrammable memory with a stored integrity value.

2. The apparatus of claim 1, wherein the integrity value is stored independently of the non-volatile reprogrammable memory.

3. The apparatus access module of claim 1, wherein the logical module comprises:

a read module for reading the data stored in the non-volatile reprogrammable memory independently of the microprocessor; and

a memory evaluation module for computing a value related to the at least a portion of the data stored in the non-volatile reprogrammable memory.

4. The apparatus of claim 3, wherein the memory evaluation module stores the value and compares the value with the integrity value.

5. The apparatus of claim 4, wherein the integrity value is stored in the logical module.

6. The apparatus of claim 4, wherein:

the integrity value is stored in a memory communicatively coupled to the microprocessor; and

the integrity value is digitally signed.

7. The apparatus of claim 4, wherein the value is a checksum.

8. The apparatus of claim 1, wherein the logical module is a state module.

9. The apparatus of claim 1, wherein the logical module is implemented in software.

10. The apparatus of claim 1, wherein the logical module is a microprocessor.

11. The apparatus of claim 1, wherein the logical module verifies all of the data stored in the non-volatile reprogrammable memory.

12. The apparatus of claim 1, wherein the logical module verifies a portion of the data stored in the non-volatile reprogrammable memory.

13. A method of verifying a content of a non-volatile reprogrammable memory communicatively coupled to a microprocessor via a first communication path, the non-volatile memory for storing microprocessor program instructions, the method comprising the steps of:

reading at least some of the data stored in the non-volatile reprogrammable memory;

computing a value related to contents of the non-volatile reprogrammable memory; and

comparing the value with a stored integrity value.

14. The method of claim 13, wherein the integrity value is stored independently from the non-volatile reprogrammable memory.

15. The method of claim 14, wherein the data stored in the non-volatile reprogrammable memory is read via a second communication path.

16. The method of claim 13, further comprising the step of transmitting a success signal if the value favorably compares with the integrity value and a failure signal if the value does not favorably compare with the integrity value.

17. The method of claim 13, wherein the value is a checksum of the data stored in the non-volatile reprogrammable memory.

18. The method of claim 13, wherein the step of comparing the value with a integrity value stored independently from the non-volatile reprogrammable memory comprises the steps of:

reading the integrity value from a second memory communicatively coupled to the microprocessor; and

comparing the read integrity value to the computed value.

19. The method of claim 14, further comprising the step of:

verifying the read integrity value by a comparison with a signature of the integrity value.

20. An apparatus for verifying a content of a non-volatile reprogrammable memory communicatively coupled to a microprocessor via a first communication path the non-volatile memory for storing microprocessor program instructions, the method comprising:

means for reading at least some of the data stored in the non-volatile reprogrammable memory via a second communication path;

means for computing a value related to contents of the non-volatile reprogrammable memory; and

means for comparing the value with a stored integrity value.

21. The apparatus of claim 20, wherein the integrity value is stored independently from the non-volatile reprogrammable memory.

22. The apparatus of claim 21, wherein the data stored in the non-volatile reprogrammable memory is read via a second communication path.

23. The apparatus of claim 20, further comprising means for transmitting a success signal if the value favorably compares with the integrity value and a failure signal if the value does not favorably compare with the integrity value.

24. The apparatus of claim 20, wherein the value is a checksum of the data stored in the non-volatile reprogrammable memory.

25. The apparatus of claim 20, wherein the means for comparing the value with a integrity value stored independently from the non-volatile reprogrammable memory comprises:

means for reading the integrity value from a second memory communicatively coupled to the microprocessor; and

means for comparing the read integrity value to the computed value.

26. The apparatus of claim 20, further comprising: means for verifying the read integrity value by a comparison with a signature of the integrity value.

27. A conditional access module, comprising:

a microprocessor;

a non-volatile reprogrammable memory communicatively coupled to the microprocessor, the non-volatile memory for storing microprocessor program instructions; and

a logical module, communicatively coupled to the non-volatile memory via a secure communication path, the logical module for verifying the data stored in the non-volatile reprogrammable memory by comparison of the contents of the non-volatile reprogrammable memory with a stored integrity value.

28. The apparatus of claim 27, wherein the secure communication path is secured by encryption.